Abstract

5   **Method of and Apparatus for Modular Multiplication**

In a method for modular multiplication using a multiplica-
tion look-ahead process for computing a multiplication
shift value and a reduction look-ahead process for comput-
10   ing a reduction shift value, a modulus is first transformed
into a transformed modulus that is greater than said
modulus. The transformation is carried out such that a pre-
determined fraction of the transformed modulus has a
higher-order digit with a first predetermined value that is
15   followed by at least one low-order digit having a second
predetermined value. During the iterative working off of
the modular multiplication using the multiplication look-
ahead process and the reduction look-ahead process, the
transformed modulus is utilized so as to obtain at the end
20   of the iteration a transformed result for the modular mul-
tiplication. Finally, the transformed result is re-
transformed by modular reduction using the original
modulus. By means of the transformation according to the
invention, iterative working off of the modular multiplica-
25   tion is simplified so that the modular multiplication can
be performed faster.

Fig. 1